CLAIMS

We claim:

1. In a computing system, a method for performing a procedure in the presence of possible failure, the procedure specifying a plurality of states including an initial state and a final state, the procedure further specifying a plurality of transitions between the states, the procedure further specifying an order of the transitions and of the states, the method comprising:

monitoring for failures;

initializing the procedure at the initial state; and

performing the procedure by executing transitions from one state to another state according to the specified order until either the final state is reached or until a failure is detected in a transition;

wherein if a failure is detected in a transition, then:

transitioning to a recovery coordination state;

transitioning from the recovery coordination state to the initial state;

re-visiting transitions from one state to another state according to the specified order until either the failed transition is reached or until a further failure is detected in a transition; and

if the failed transition is reached without further failure, then executing transitions from one state to another state according to the specified order from the failed transition until either the final state is reached or until a further failure is detected in a transition.

2. The method of claim 1 wherein the computing system comprises a first computing device; and

wherein the transitions specified by the procedure are all performed on the first computing device.

3. The method of claim 1 wherein the computing system comprises a plurality of computing devices;

wherein at least one transition specified by the procedure is executed on a first computing device; and

wherein at least one other transition specified by the procedure is executed on a second computing device.

4. The method of claim 3 wherein the procedure moves a resource from the first computing device to the second computing device.

5. The method of claim 4 wherein each of the first and the second computing devices comprises a moveaway flag.

6. The method of claim 3 wherein the computing system comprises a third computing device;

wherein the third computing device comprises a target resource server flag and a current resource server flag; and

wherein at least one transition specified by the procedure atomically changes values of both the target resource server flag and the current resource server flag.

7. The method of claim 6 wherein the first computing device is a resource server;

wherein the second computing device is a resource server; and

wherein the third computing device is a directory server.

8. The method of claim 1 wherein each transition specified by the procedure is idempotent.

9. The method of claim 1 wherein at least one state specified by the procedure specifies a plurality of substates and transitions between the substates.

10. The method of claim 1 wherein transitioning to a recovery coordination state comprises generating an error message.

11. The method of claim 1 wherein, for at least one transition before the failed transition, re-visiting the transition comprises skipping the transition.

12. The method of claim 1 wherein, for at least one transition before the failed transition, re-visiting the transition comprises re-executing the transition.

13. The method of claim 12 wherein re-executing the transition comprises receiving an error message that the transition has already been performed.

14. A computer-readable medium containing computer-executable instructions for performing a method for performing a procedure in the presence of possible failure, the procedure specifying a plurality of states including an initial state and a final state, the procedure further specifying a plurality of transitions between the states, the procedure further specifying an order of the transitions and of the states, the method comprising:

monitoring for failures;

initializing the procedure at the initial state; and

performing the procedure by executing transitions from one state to another state according to the specified order until either the final state is reached or until a failure is detected in a transition;

wherein if a failure is detected in a transition, then:

transitioning to a recovery coordination state;

transitioning from the recovery coordination state to the initial state;

re-visiting transitions from one state to another state according to the specified order until either the failed transition is reached or until a further failure is detected in a transition; and

if the failed transition is reached without further failure, then executing transitions from one state to another state according to the specified order from the failed transition until either the final state is reached or until a further failure is detected in a transition.

15. In a computing system comprising a directory server, a first resource server, and a second resource server, the directory server comprising a current resource server flag and a target resource server flag, the first and second resource servers each comprising a moveaway flag, a method for moving a resource from the first resource server to the second resource server, the method comprising the following elements:

setting the directory server's current resource server flag to indicate the first resource server;

setting the directory server's target resource server flag to not indicate any resource server;

setting the first resource server's moveaway flag to FALSE;

setting the directory server's target resource server flag to indicate the second resource server;

setting the first resource server's moveaway flag to TRUE;

copying the resource from the first resource server to the second resource server;

setting the second resource server's moveaway flag to FALSE;

setting the directory server's current resource server flag to indicate the second resource server; and

setting the directory server's target resource server flag to not indicate any resource server.

16. The method of claim 15 wherein the directory server and the first resource server are the same server.

17. The method of claim 15 wherein the elements of the method are idempotent operations.

18. The method of claim 15 further comprising:

deleting the resource from the first resource server.

19. The method of claim 15 further comprising:

monitoring for failures;

wherein if a failure is detected in an element of the method, then:

coordinating a failure recovery;

re-visiting elements of the procedure until either the failed element is reached or until a further failure is detected; and

if the failed element is reached without further failure, then performing elements from the failed element until either the final element is successfully performed or until a further failure is detected.

20. The method of claim 19 wherein coordinating a failure recovery comprises generating an error message.

21. The method of claim 19 wherein, for at least one element before the failed element, re-visiting the element comprises skipping the element.

22. The method of claim 19 wherein, for at least one element before the failed element, re-visiting the element comprises re-executing the element.

23. The method of claim 22 wherein re-executing the element comprises receiving an error message that the element has already been performed.

24. A computer-readable medium containing computer-executable instructions for performing a method for moving a resource from a first resource server to a second resource server, the first and second resource servers each comprising a moveaway flag, the method comprising the following elements:

setting the directory server's current resource server flag to indicate the first resource server;

setting the directory server's target resource server flag to not indicate any resource server;

setting the first resource server's moveaway flag to FALSE;

setting the directory server's target resource server flag to indicate the second resource server;

setting the first resource server's moveaway flag to TRUE;

copying the resource from the first resource server to the second resource server;

setting the second resource server's moveaway flag to FALSE;

setting the directory server's current resource server flag to indicate the second resource server; and

setting the directory server's target resource server flag to not indicate any resource server.

25. In a computing system comprising a directory server computing device, a first resource server computing device, and a second resource server computing device, the directory server comprising a current resource server flag and a target resource server flag, the first and second resource servers each comprising a moveaway flag, a method for the directory server to move a resource from the first resource server to the second resource server, the method comprising the following elements:

setting the directory server's current resource server flag to indicate the first resource server;

setting the directory server's target resource server flag to not indicate any resource server;

setting the directory server's target resource server flag to indicate the second resource server;

requesting that the first resource server set its moveaway flag to TRUE;

copying the resource from the first resource server to the second resource server;

requesting that the second resource server set its moveaway flag to FALSE;

setting the directory server's current resource server flag to indicate the second resource server; and

setting the directory server's target resource server flag to not indicate any resource server.

26. The method of claim 25 wherein the directory server and the first resource server are the same server.

27. The method of claim 25 wherein the elements of the method are idempotent operations.

28. The method of claim 25 wherein copying the resource comprises requesting that the first resource server send a copy of the resource to the second resource server.

29. The method of claim 25 further comprising:

requesting that the first resource server delete the resource.

30. The method of claim 25 further comprising:

monitoring for failures;

wherein if a failure is detected in an element of the method, then:

coordinating a failure recovery;

re-visiting elements of the procedure until either the failed element is reached or until a further failure is detected; and

if the failed element is reached without further failure, then performing elements from the failed element until either the final element is successfully performed or until a further failure is detected.

31. The method of claim 30 wherein coordinating a failure recovery comprises generating an error message.

32. The method of claim 30 wherein, for at least one element before the failed element, re-visiting the element comprises skipping the element.

33. The method of claim 30 wherein, for at least one element before the failed element, re-visiting the element comprises re-executing the element.

34. The method of claim 33 wherein re-executing the element comprises receiving an error message that the element has already been performed.

35. A computer-readable medium containing computer-executable instructions for performing a method for a directory server to move a resource from a first resource server to a second resource server, the directory server comprising a current resource server flag and a target resource server flag, the first and second resource servers each comprising a moveaway flag, the method comprising the following elements:

setting the directory server's current resource server flag to indicate the first resource server;

setting the directory server's target resource server flag to not indicate any resource server;

setting the directory server's target resource server flag to indicate the second resource server;

requesting that the first resource server set its moveaway flag to TRUE;

copying the resource from the first resource server to the second resource server;

requesting that the second resource server set its moveaway flag to FALSE;

setting the directory server's current resource server flag to indicate the second resource server; and

setting the directory server's target resource server flag to not indicate any resource server.

36. In a computing system comprising a first resource server and a second resource server, the first resource server comprising a moveaway flag, a method for the first resource server to move a resource to the second resource server, the method comprising the following elements:

setting the first resource server's moveaway flag to FALSE;

setting the first resource server's moveaway flag to TRUE; and

copying the resource from the first resource server to the second resource server.

37. The method of claim 36 wherein the elements of the method are idempotent operations.

38. The method of claim 36 further comprising:

deleting the resource from the first resource server.

39. A computer-readable medium containing computer-executable instructions for performing a method for a first resource server to move a resource to a second resource server, the first resource server comprising a moveaway flag, the method comprising the following elements:

setting the first resource server's moveaway flag to FALSE;

setting the first resource server's moveaway flag to TRUE; and

copying the resource from the first resource server to the second resource server.

40. In a computing system comprising a first resource server and a second resource server, the second resource server comprising a moveaway flag, a method for the second resource server to receive a resource from the first resource server, the method comprising the following elements:

receiving the resource from the first resource server; and

setting the second resource server's moveaway flag to FALSE.

41. The method of claim 40 wherein the elements of the method are idempotent operations.

42. A computer-readable medium containing computer-executable instructions for performing a method for a second resource server to receive a resource from a first resource server, the second resource server comprising a moveaway flag, the method comprising the following elements:

receiving the resource from the first resource server; and

setting the second resource server's moveaway flag to FALSE.

43. A computer-readable medium containing a resource movement data structure, the resource movement data structure comprising:

a first data field containing data representing a current resource server flag; and

a second data field containing data representing a target resource server flag.

44. The computer-readable medium of claim 43 wherein the resource movement data structure further comprises:

a third data field containing data indicating a failed element of a resource movement method.

45. The computer-readable medium of claim 43 wherein the resource movement data structure further comprises:

a third data field containing data representing a Boolean moveaway flag; and

a fourth data field containing data representing a resource.

46. A computer-readable medium containing a resource movement data structure, the resource movement data structure comprising:

a first data field containing data representing a Boolean moveaway flag; and

a second data field containing data representing a resource.

47. A computer-readable medium containing a procedure data structure, the procedure data structure comprising:

a first data field containing data representing a plurality of states of a procedure, the plurality of states comprising an initial state and a final state;

a second data field containing data representing a plurality of transitions between the states of the procedure;

a third data field containing data representing an order of the transitions and of the states of the procedure;

a fourth data field containing data representing a recovery coordination state; and

a fifth data field containing data representing a failed transition of the procedure.

48. The computer-readable medium of claim 47 wherein each of the plurality of transitions is idempotent.

49. The computer-readable medium of claim 47 wherein at least one of the plurality of states comprises a plurality of substates and transitions between the substates.

50. A resource server system, the system comprising:

a directory server comprising a current resource server flag and a target resource server flag;

a first resource server comprising a Boolean moveaway flag and a resource; and

a second resource server comprising a Boolean moveaway flag.

51. The resource server system of claim 50 wherein the directory server and the first resource server are the same server.